AMENDMENTS TO THE CLAIMS

1. (currently amended) A method of controlling access of network management requests directed to one or more network devices that participate in a virtual private network, the method comprising the computer-implemented steps of:

receiving a request, from a first network device participating in a virtual private network, to carry out a management protocol operation that involves one or more managed objects associated with one or more second network devices participating in the virtual private network;

determining an identifier of [[a]] the virtual private network in the request to carry out the management protocol operation;

identifying, among a plurality of managed objects, a subset of objects that requests associated with the virtual private network are permitted to access; and

in response to the request, providing ~~the request with~~ to the first network device access to only the subset of objects.

2. (original) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects.

3. (previously presented) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects, in the form of one or more entries in a view-based access control model table that associate

SNMPv3 securityName values to corresponding MIB (Management Information Base) Views.

4. (previously presented) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks.

5. (original) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects, and wherein the steps of identifying a subset of objects and providing the request with access comprise the steps of.

determining whether the identifier from the request is in the mapping;

when the identifier from the request is in the mapping:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the mapping, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

6. (previously presented) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects, in the form of one or more entries in a view-based access control model table that associate security name values to corresponding MIB (Management Information Base) Views, and wherein the steps of identifying a subset of objects and providing the request with access comprise the steps of:

determining whether the identifier from the request is in the view-based access control model table;

when the identifier from the request is in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more MIB Views referenced in the view-based access control model table, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

7. (previously presented) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding

MIB Views represent access control policies applicable to the associated virtual private networks, and wherein the steps of identifying a subset of objects and providing the request with access comprise the steps of:

determining whether the identifier from the request is in the view-based access control model table;

when the identifier from the request is in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more MIB Views referenced in the view-based access control model table, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

8. (original) A method as recited in Claim 1, further comprising the steps of:

providing, at a network management station that is communicatively coupled to the network devices, a mapping of a plurality of virtual private network identifiers to SNMPv3 securityNames;

providing, at the network management station, an executable process that associates a virtual private network identifier with each SNMP request that is issued by the network management station to the network devices.

9. (currently amended) A method of controlling access of network management requests directed to one or more network devices that participate in a virtual private network, the method comprising the computer-implemented steps of:

receiving, from a network device participating in a virtual private network, a request to carry out a management protocol operation, wherein the request contains an identifier of the virtual private network ~~identifier~~ in a security name value;

extracting the security name value, which identifies the virtual private network, and determining a protocol operation that is embodied in the request;

using a view-based access control model, matching the security name value, which identifies the virtual private network, to a management information base view that corresponds to the requested operation;

processing the requested operation only if access is allowed to managed objects, in the management information base, that are associated with one or more network devices participating in the virtual private network, based on the ~~matching~~ management information base view matching the security name value that identifies the virtual private network.

10. (original) A method as recited in Claim 9, further comprising the steps of:

determining whether the request can be satisfied;

extracting the security name value from a context string in the request.

11. (original) A method as recited in Claim 10, wherein the matching step further comprises the steps of:

determining whether the security name is in a view-based access control model table;

rejecting and returning the request when the security name is not found in the view-based access control model table.

12. (original) A method as recited in Claim 10, further comprising the steps of:

determining whether the security name is in a view-based access control model table;

when the security name is found in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the view-based access control model table, determining whether the protocol operation is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

13. (previously presented) The method as recited in Claim 10, further comprising the steps of:

determining whether the security name is in a view-based access control model table;

when the security name is found in the view-based access control model table:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the view-based access control model table, determining whether the protocol operation is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable;

determining whether a virtual private network identifier is referenced in the request, processing the request using managed information objects in a default view when no virtual private network identifier is referenced in the request, and processing the request using management information objects in a view corresponding to the virtual private network identifier only when a virtual private network identifier is referenced in the request.

14. (currently amended) A computer-readable medium carrying one or more sequences of instructions for controlling access of network management requests directed to one or more network devices that participate in a virtual private network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving a request, from a first network device participating in a virtual private network, to carry out a management protocol operation that involves one or more managed objects associated with one or more second network devices participating in the virtual private network;

determining an identifier of [[a]] the virtual private network in the request to carry out the management protocol operation;

identifying, among a plurality of managed objects, a subset of objects that requests associated with the virtual private network are permitted to access; and

in response to the request, providing ~~the request with~~ to the first network device access to only the subset of objects.

15. (original) A computer-readable medium as recited in Claim 14, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects.

16. (previously presented) A computer-readable medium as recited in Claim 14, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects, in the form of one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views.

17. (previously presented) A computer-readable medium as recited in Claim 14, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of providing, at one of the network devices, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual

private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks.

18. (original) A computer-readable medium as recited in Claim 14, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects, and wherein the steps of identifying a subset of objects and providing the request with access comprise the steps of.

determining whether the identifier from the request is in the mapping;

when the identifier from the request is in the mapping:

identifying a management information base variable referenced in the request;

based on one or more views referenced in the mapping, determining whether a protocol operation of the request is allowed for the variable;

dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

19. (currently amended) An apparatus for controlling access of network management requests directed to one or more network devices that participate in a virtual private network, comprising:

means for receiving a request, from a first network device participating in a virtual private network, to carry out a management protocol operation that involves

one or more managed objects associated with one or more second network devices participating in the virtual private network;

means for determining an identifier of [[a]] the virtual private network in the request to carry out the management protocol operation;

means for identifying, among a plurality of managed objects, a subset of objects that requests associated with the virtual private network are permitted to access; and

means for providing ~~the request with~~ to the first network device access to only the subset of objects.

20. (currently amended) An apparatus controlling access of network management requests directed to one or more network devices that participate in a virtual private network, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a request, from a first network device participating in a virtual private network, to carry out a management protocol operation that involves one or more managed objects associated with one or more second network devices participating in the virtual private network;

determining an identifier of [[a]] the virtual private network in the request to carry out the management protocol operation;

identifying, among a plurality of managed objects, a subset of objects that requests associated with the virtual private network are permitted to access; and

in response to the request, providing ~~the request with~~ to the first network device access to only the subset of objects.

21. (previously presented) A method of controlling access of network management requests directed to one or more network devices that participate in one or more virtual private networks, the method comprising the computer-implemented steps of:

receiving a request to carry out a SNMP (Simple Network Management Protocol) operation directed to one or more managed objects from a MIB (Management Information Base) associated with one or more network devices that participate in multiple virtual private networks;

determining, from the request, an identifier of a particular virtual private network of the multiple virtual private networks;

identifying, among a plurality of managed objects from a MIB associated with a network device from the one or more network devices that participate in the multiple virtual private networks, a subset of managed objects that requests associated with the particular virtual private network are permitted to access; and

in response to the request, providing access to only the subset of managed objects.